Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method comprising:

establishing a protected communications channel with a trusted code module executing in a trusted execution environment in an open platform of a computing system, the computing system providing subscriber identity module (SIM) authentication, authorization, and accounting (SIM AAA) capabilities without use of a discrete hardware SIM device;

provisioning SIM secret data to the computing system over the protected communications channel; and

providing access to a service ~~protected memory~~ by the ~~said~~ open platform of the computing system using the ~~said~~ SIM AAA capabilities in the trusted execution environment of the computing system.

2. (Original) The method of claim 1 wherein provisioning SIM secret data includes provisioning at least one of identity secrets, key secrets, information to initialize data objects, information to initialize operator-specific cryptography algorithms, and information to install or update applications, parameters, tools or utilities.

3. (Original) The method of claim 1 wherein establishing a protected communications channel includes using a protected key exchange mechanism.

4. (Original) The method of claim 3 wherein provisioning SIM secret data includes encrypting the SIM secret data.

5. (Currently Amended) A method comprising:

~~providing access to a trusted environment in an open platform of a computer system;~~

establishing a protected communications channel with a trusted code module executing in a protected execution environment in an open platform of a computing system;

using subscriber identity module (SIM) capabilities provided by the computing system in the protected execution environment without a discrete hardware SIM device for user authorization, authentication and accounting in association with a subscription account; and

providing a subscription account service for access by the open platform of the computing system using the SIM capabilities in the protected execution environment of the computing system.

6. (Currently Amended) The method of claim 5 wherein providing the subscription account service includes providing a wireless network access account.

7. (Original) The method of claim 6 wherein using SIM capabilities provided by a computing system includes using SIM capabilities provided by a laptop computing system.

8. (Currently Amended) The method of claim 5 wherein providing the subscription account service includes providing a wired network access account.

9. (Currently Amended) The method of claim 5 wherein using SIM capabilities includes using the ~~a~~ protected execution environment provided by a laptop computing system.

10. (Currently Amended) The method of claim 5 wherein providing the subscription account service includes providing location-based services.

11. (Currently Amended) A tangible computer-accessible storage medium storing information, that when accessed by a computing system causes the computing system to:

establish a protected communications channel with a trusted code module executing in a trusted execution environment in an open platform of a computing system, the computing system to provide subscriber identity module (SIM) authentication, authorization, and accounting (SIM AAA) capabilities without use of a discrete hardware SIM device;

provision SIM secret data to the computing system over the protected communications channel; and

provide ~~providing~~ access to a service ~~protected memory~~ by the ~~said~~ open platform of the computing system using said SIM AAA capabilities in the trusted execution environment of the computing system.

12. (Previously Presented) The tangible computer-accessible storage medium of claim wherein provisioning SIM secret data includes provisioning at least one of identity secrets, key secrets, information to initialize data objects, information to initialize operator-specific cryptography algorithms, and information to install or update applications, parameters, tools or utilities.

13. (Previously Presented) The tangible computer-accessible storage medium of claim wherein provisioning includes encrypting the secret data prior to providing the secret data to the computing system.

14. (Previously Presented) The tangible computer-accessible storage medium of claim wherein establishing a protected communications channel includes participating in a bilateral key exchange.

15. (Previously Presented) The tangible computer-accessible storage medium of claim wherein establishing a protected communications channel includes receiving authentication information from the computing system.

16. (Currently Amended) A method comprising:

establishing a protected communications channel with a trusted code module executing in a trusted execution environment in an open platform of a computing system;

authenticating and authorizing a user of a subscription account at least in part by using Subscriber Identity Module (SIM) compliant authentication and authorization capabilities on a trusted execution environment in the ~~an~~ open platform of the ~~a~~ computing system that provides the SIM-compliant authentication and authorization capabilities without use of a discrete SIM hardware device; and

providing user access to the subscription account upon receipt of predetermined credentials.

17. (Original) The method of claim 16 wherein providing user access to the subscription account includes providing user access to a wireless network account.

18. (Original) The method of claim 17 wherein providing user access to wireless network account includes providing access to one of a GSM/GPRS network, a 3G network and a Personal Handyphone Network.

19. (Original) The method of 16 wherein providing user access to the subscription account includes providing user access to a location-based services account.

20. (Currently Amended) An apparatus comprising:

a server having access to a network; and

a provisioning module stored on the server, the provisioning module, when executed by the provisioning server, to establish a protected communications channel with a trusted code module executing in a trusted execution environment in an open platform of a computing system and participate in provisioning Subscriber Identity Module (SIM) secret data from the server to the ~~a~~ trusted execution environment ~~in an open platform of a computer system to the computing system~~, the computing system to provide SIM-compliant authentication, authorization, and accounting capabilities without use of a discrete hardware SIM device, and the server to provide access to a service by the computing system using the SIM-compliant authentication, authorization and accounting capabilities in the trusted execution environment of the computing system.

21. (Original) The apparatus of claim 20 wherein the network is one of a GSM/GPRS, 3G, Personal Handyphone System (PHS) and a CDMA network.

22. (Original) The apparatus of claim 20 wherein the network is a wireless network.

23. (Original) The apparatus of claim 20 wherein the network is a wired network.

24. (Original) The apparatus of claim 20 wherein the provisioning module, when executed by the server, further operates to encrypt the SIM secret data to be provided to the computing system.

25. (Original) The apparatus of claim 24 wherein the provisioning module, when executed by the server, further operates to participate in a bilateral key exchange with the computing system over the network.

26. (Original) The apparatus of claim 20 wherein the computing system is further to store the SIM secret data in an encrypted format on a mass storage device of the computing system.

27. (Original) The apparatus of claim 26 wherein the computing system is further to store an encrypted bulk encryption key to be used to decrypt the encrypted SIM secret data.

28. (Original) The apparatus of claim 27 wherein the computing system further includes a hardware token to provide a second key to encrypt the bulk encryption key.

29. (Currently Amended) The apparatus of claim 20 wherein the server is further to control access by the computing system to a service~~, the server to provide access to the service by the computing system~~ upon authorization and authentication of the computing system using the SIM-compliant authentication, authorization and accounting capabilities.